R E P U B L I Q U E . F R A N Ç A I S E

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 0 1 MARS 2001

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS cedex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30
http://www.inpi.fr

DB 267161000
ETABLISSEMENT PUBLIC NATIONAL CREE PAR LA LOI N° 51-444 DU 19 AVRIL 1951

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11354*01

REQUÊTE EN DÉLIVRANCE 1/2

Cet imprimé est à remplir lisiblement à l'encre noire

DB 540 W /260899

Réservé à l'INPI

REMISE DES PIÈCES
DATE 28 MARS 2000
LIEU 75 INPI PARIS

N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0003919

DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 28 MARS 2000

Vos références pour ce dossier *(facultatif)* 015515 (GEM846)

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

Cabinet BALLOT-SCHMIT
16, Avenue du Pont Royal
94230 CACHAN
FRANCE

MK/PL

Confirmation d'un dépôt par télécopie ☐ N° attribué par l'INPI à la télécopie

2 NATURE DE LA DEMANDE	Cochez l'une des 4 cases suivantes
Demande de brevet	☒
Demande de certificat d'utilité	☐
Demande divisionnaire	☐
Demande de brevet initiale	N° Date / /
ou demande de certificat d'utilité initiale	N° Date / /
Transformation d'une demande de brevet européen *Demande de brevet initiale*	☐ N° Date / /

3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)

Procédé de génération de clés électroniques à partir de nombres entiers premiers entre eux et dispositif de mise en oeuvre du procédé.

4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE	
	Pays ou organisation Date / / N°
	Pays ou organisation Date / / N°
	Pays ou organisation Date / / N°
	☐ **S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»**

5 DEMANDEUR		☐ **S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»**
Nom ou dénomination sociale		GEMPLUS
Prénoms		
Forme juridique		Société Anonyme
N° SIREN		
Code APE-NAF		
Adresse	Rue	Avenue du Pic de Bertagne Parc d'Activités de la Plaine de Jouques
	Code postal et ville	13420 GEMENOS
Pays		FRANCE
Nationalité		Française
N° de téléphone *(facultatif)*		
N° de télécopie *(facultatif)*		
Adresse électronique *(facultatif)*		

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE 2/2

Réservé à l'INPI

REMISE DES PIÈCES
DATE 28 MARS 2000
LIEU 75 INPI PARIS

N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0003919

DB 540 W /260899

Vos références pour ce dossier : *(facultatif)*	015515 (GEM846)
6 MANDATAIRE	
Nom	BORIN
Prénom	Lydie
Cabinet ou Société	Cabinet BALLOT-SCHMIT
N °de pouvoir permanent et/ou de lien contractuel	
Adresse — Rue	16, Avenue du Pont Royal
Adresse — Code postal et ville	94230 | CACHAN
N° de téléphone *(facultatif)*	01 49 69 91 91
N° de télécopie *(facultatif)*	01 49 69 91 90
Adresse électronique *(facultatif)*	
7 INVENTEUR (S)	
Les inventeurs sont les demandeurs	☐ Oui ☒ Non **Dans ce cas fournir une désignation d'inventeur(s) séparée**
8 RAPPORT DE RECHERCHE	**Uniquement pour une demande de brevet (y compris division et transformation)**
Établissement immédiat ou établissement différé	☒ ☐
Paiement échelonné de la redevance	**Paiement en deux versements, uniquement pour les personnes physiques** ☐ Oui ☒ Non
9 RÉDUCTION DU TAUX DES REDEVANCES	**Uniquement pour les personnes physiques** ☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)* ☐ Requise antérieurement à ce dépôt *(joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence)* :
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes	

10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE
(Nom et qualité du signataire)

BORIN Lydie
Mandataire N° 94-0506
Cabinet BALLOT-SCHMIT

VISA DE LA PRÉFECTURE OU DE L'INPI

P. BERNOUIS

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11235*02

DÉSIGNATION D'INVENTEUR(S) Page N° .1./.1.

(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 W /260899

Vos références pour ce dossier *(facultatif)*	015515 (GEM846)
N° D'ENREGISTREMENT NATIONAL	0003919

TITRE DE L'INVENTION (200 caractères ou espaces maximum)

Procédé de génération de clés électroniques à partir de nombres entiers premiers entre eux et dispositif de mise en oeuvre du procédé.

LE(S) DEMANDEUR(S) :

GEMPLUS (S.A.)

Avenue du Pic de Bertagne
Parc d'Activités de la Plaine de Jouques
13420 GEMENOS
FRANCE

DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).

Nom		PAILLIER
Prénoms		Pascal
Adresse	Rue	domicilié : au Cabinet BALLOT-SCHMIT 16, Avenue du Pont Royal
	Code postal et ville	94230 CACHAN
Société d'appartenance *(facultatif)*		
Nom		
Prénoms		
Adresse	Rue	
	Code postal et ville	
Société d'appartenance *(facultatif)*		
Nom		
Prénoms		
Adresse	Rue	
	Code postal et ville	
Société d'appartenance *(facultatif)*		

DATE ET SIGNATURE(S)
DU (DES) DEMANDEUR(S)
OU DU MANDATAIRE
(Nom et qualité du signataire)

BORIN Lydie
Mandataire N° 94-0506
Cabinet BALLOT-SCHMIT

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

015515 (GEM846)
PAILLIER Pascal

PROCEDE DE GENERATION DE CLES ELECTRONIQUES A PARTIR DE NOMBRES ENTIERS PREMIERS ENTRE EUX ET DISPOSITIF DE MISE EN ŒUVRE DU PROCEDE.

L'invention concerne un procédé de génération de clés électroniques à partir de nombres entiers premiers entre eux et un dispositif de mise en œuvre du procédé.

L'invention s'applique tout particulièrement à des protocoles de cryptographie à clé publique utilisés pour le cryptage d'informations et/ou l'authentification entre deux entités et/ou la signature électronique de messages.

Elle s'applique en particulier à des protocoles de cryptographie à clé publique tels que le protocole RSA (Rivest Shamir et Adelman), El Gamal, Schnorr, Fiat Shamir.

Dans le cas de telles applications on fait, en effet appel à la génération de grands nombres entiers (pouvant être par exemple être supérieurs ou égaux à 512 bits) pour former une ou plusieurs clés du protocole. Une condition est imposée pour le choix de ces nombres afin qu'ils restent secrets c'est qu'ils doivent être co-premiers ou premiers entre eux.

De façon pratique, le dispositif électronique qui désire générer de tels nombres en vue par exemple de mettre en œuvre un protocole de cryptographie, opère de manière connue de la façon suivante :

-Prendre un nombre entier a (choisi parmi un ensemble de nombres entiers prédéterminés, ou tiré aléatoirement),

-Tirer de façon aléatoire un deuxième nombre entier b,

-Effectuer une opération de vérification de la co-primalité entre les nombres a et b. Cette opération permet de vérifier que les deux nombres entiers a, b obtenus sont premiers entre eux. Elle est réalisée par l'unité centrale du dispositif. L'unité centrale calcule pour cela le plus grand commun diviseur (pgcd) entre ces deux nombres et vérifie que le résultat est égal à 1. En effet on rappelle que deux nombres sont co-premiers si et seulement si leur plus grand commun diviseur est égal à 1.

Il existe pour cela plusieurs techniques bien connues d'implémentation du calcul du pgcd de deux nombres à l'aide d'un microprocesseur.

On peut citer à titre d'exemple les techniques telles que celle du « Binary GCD », du « Extended GCD » ou la technique de Lehmer. Malgré une complexité asymptotique excellente (c'est-à-dire pour des nombres de taille extrêmement grande), ces techniques s'avèrent à la fois difficile à programmer sur des dispositifs portables de type carte à microprocesseur (car complexes) et de performances médiocres pour des nombres de grandes de tailles usuelles (512 bits) qui tendent à ce jour à devenir supérieures à savoir 1024 bits et plus.

L'invention a pour but de remédier à cet inconvénient. Elle a plus particulièrement pour objet un procédé de génération de clés électroniques à partir de deux nombres entiers a, b, le procédé comprenant une étape de vérification de la co-primalité desdits nombres a, b, principalement caractérisé en ce que cette étape de vérification comprend les opérations suivantes :

A) - calcul de l'exponentiation, modulaire $a^{\lambda(b)} \bmod b$, où λ est la fonction de Carmichael,

B) - vérification que cette exponentiation modulaire est égale à 1,

et en ce que :

C) - on retient le couple a, b lorsque l'égalité est vérifiée et on réitère avec un autre couple dans le cas contraire.

Selon une autre caractéristique :

- on choisit un nombre entier b d'une longueur donnée et on le mémorise,
- on tire au hasard un nombre entier a,
- on calcule $a^{\lambda(b)} \text{mod} b$
- on vérifie que $a^{\lambda(b)} = 1 \text{ mod} b$ (ou $a^{\lambda(b)} \text{mod} b = 1$),
- on mémorise le nombre a dans le cas où l'égalité est vérifiée,
- on réitère les étapes précédentes avec un autre nombre a dans le cas contraire.

Selon une autre caractéristique, dans le cas où le nombre b est donné au préalable, on pré calcule la valeur $\lambda(b)$ et on la stocke en mémoire.

L'invention s'applique aux procédés de génération de clés cryptographiques RSA ou El Gamal ou Schnorr.

L'invention a également pour objet un dispositif électronique portable comprenant un processeur arithmétique et une mémoire de programme associée, apte à effectuer des exponentiations modulaires, principalement caractérisé en ce qu'il comprend un programme de vérification de co-primalité de nombres entiers de longueur donnée qui effectue les opérations suivantes :

A) - calcul de l'exponentiation modulaire $a^{\lambda(b)} \text{mod} b$, où λ est la fonction de Carmichael,

B) - vérification que cette exponentiation modulaire est égale à 1,

et en ce que :

C) le processeur arithmétique stocke le couple a, b lorsque l'égalité est vérifiée et réitère avec un autre couple dans le cas contraire.

Selon une autre caractéristique, dans le cas où le nombre b est donné au préalable, on pré calcule la valeur $\lambda(b)$ et on la stocke en mémoire.

Avantageusement le dispositif électronique portable, est constitué par une carte à puce à microprocesseur.

D'autres particularités et avantages de l'invention apparaîtront clairement à la lecture de la description qui est faite ci-après et qui est donnée à titre d'exemple non limitatif et en regard des dessins annexés sur lesquels :

- la figure 1, représente le schéma de principe d'un dispositif électronique portable tel qu'une carte à puce mettant en œuvre le procédé selon l'invention,
- la figure 2, représente le schéma d'un exemple de réalisation de le mise en œuvre du procédé selon l'invention.

Dans la description qui va suivre, on a pris comme exemple de dispositif électronique portable celui des cartes à puces à microprocesseur et on parlera pour simplifier de cartes à microprocesseur.

Dans le cas de la mise en œuvre de protocoles de cryptographie tels que le RSA par exemple, il est comme on la dit nécessaire de déterminer un couple de nombres entiers de longueur donnée, premiers entre eux servant à la génération de clés électroniques du protocole.

Afin de s'assurer que les nombres générés sont premiers entre eux une étape de vérification de coprimalité est réalisée par la carte à microprocesseur

qui met en œuvre le procédé de génération de clés pour le protocole de cryptographie.

En pratique dans le protocole RSA, les deux nombres entiers a, b, restent secrets, ils doivent être premiers entre eux et ont une longueur fixée généralement de 512 bits ou 1024 bits chacun. Selon ce même exemple, un des deux nombres b est un nombre entier choisi à l'avance et stocké parmi un ensemble de nombres générés par la carte à microprocesseur tandis que l'autre nombre a est généré de manière aléatoire par la carte à microprocesseur à l'exécution du protocole. A cette fin, la carte à microprocesseur possède un générateur de nombres aléatoires, capable de fournir un nombre entier de la taille désirée.

On a donc représenté sur la figure 1 le schéma fonctionnel d'une carte à microprocesseur susceptible de mettre en œuvre le procédé selon l'invention.

La carte C comporte une unité principale de traitement 1, des mémoires de programmes 3 et 4 et une mémoire de travail (non représentée), associées à l'unité 1. La carte comporte également un processeur arithmétique 2 capable d'effectuer des calculs d'exponentiation modulaire. Il pourra s'agir par exemple de circuits tels que le circuit ST16CF54 commercialisé par la société STMicroelectronics ou 83C852/5 de la société Philips. La carte possède également un générateur de nombres entiers aléatoires 5.

Selon l'invention, l'opération de vérification de la co-primalité des nombres entiers a et b est réalisée par les étapes A et B indiquées sur le schéma de la figure 2, avec l'étape de retenue du couple a, b pour générer une clé électronique dans le cas où ces nombres sont premiers entre eux. En pratique cette étape consiste à stocker le couple a, b dans la mémoire sécuri-

sée 6 (non accessible de l'extérieur) du processeur arithmétique 2.

Avant de décrire l'exemple d'implémentation du procédé selon l'invention dans le cas du protocole RSA, on rappelle que la fonction λ est la fonction de Carmichael et que cette fonction est définie par la relation suivante :

$\lambda(b) = PPCM(\lambda(p^{\delta_1}), \quad , (\lambda(p^{\delta_k}))$,

dans laquelle PPCM désigne le plus petit commun multiple,

dans laquelle $b = \Pi p_i^{\delta_i}$ où chaque p_i est un nombre premier et chaque δ_i un entier positif non nul et $1<i<k$.

Dans l'exemple illustré du protocole de cryptographie RSA on procède aux étapes suivantes :

- stockage du nombre entier b choisi de longueur donnée fixée, (10)
- calcul de $\lambda(b)$ (20)
- stockage du nombre $\lambda(b)$ (30)

Ces étapes peuvent être préalables aux étapes qui suivent dans la mesure où b serait connu d'avance. Dans ce cas la valeur $\lambda(b)$ pré calculée sera stockée en mémoire sécurisée 6 du processeur arithmétique 5.

- tirage d'un nombre entier aléatoire a (40)
- calcul de $a^{\lambda(b)} \text{mod} b$ (50)
- comparaison de $a^{\lambda(b)} \text{mod} b$ à 1 (60)
- s'il y a égalité, stockage du couple (a, b) pour générer une clé du protocole de cryptographie, (70)
- s'il n'y a pas d'égalité (80)

réitération des étapes précédentes à partir du tirage d'un nouveau nombre entier a.

REVENDICATIONS

1. Procédé de génération de clés électroniques à partir de deux nombres entiers a, b, le procédé comprenant une étape de vérification de la co-primalité desdits nombres a, b, caractérisé en ce que cette étape de vérification comprend les opérations suivantes :

A) - calcul de l'exponentiation, modulaire $a^{\lambda(b)}$modb, où λ est la fonction de Carmichael,

B) - vérification que cette exponentiation modulaire est égale à 1,

et en ce que :

C) - on retient le couple a, b lorsque l'égalité est vérifiée et on réitère avec un autre couple dans le cas contraire.

2. Procédé de génération de clés électroniques selon la revendication 1, caractérisé en ce que :

- on choisit un nombre entier b d'une longueur donnée et on le mémorise,
- on tire au hasard un nombre entier a,
- on calcule $a^{\lambda(b)}$modb
- on vérifie que $a^{\lambda(b)} = 1$ modb (ou $a^{\lambda(b)}$modb = 1),
- on mémorise le nombre a dans le cas où l'égalité est vérifiée,
- on réitère les étapes précédentes avec un autre nombre a dans le cas contraire.

3. Procédé de génération de clés électroniques selon la revendication 1, caractérisé en ce que dans le cas où le nombre b est donné au préalable, on pré calcule la valeur $\lambda(b)$ et on la stocke en mémoire.

4. Procédé de génération de clés cryptographiques RSA ou El Gamal ou Schnorr, caractérisé en ce qu'il met en œuvre le procédé selon l'une quelconque des revendications précédentes.

5. Dispositif électronique portable comprenant un processeur arithmétique et une mémoire de programme associée, apte à effectuer des exponentiations modulaires, caractérisé en ce qu'il comprend un programme de vérification de co-primalité de nombres entiers de longueur donnée qui effectue les opérations suivantes :

A) - calcul de l'exponentiation modulaire $a^{\lambda(b)} \mathrm{mod} b$, où λ est la fonction de Carmichael,

B) - vérification que cette exponentiation modulaire est égale à 1,

et en ce que :

D) le processeur arithmétique stocke le couple a, b lorsque l'égalité est vérifiée et réitère avec un autre couple dans le cas contraire.

6. Dispositif électronique portable selon la revendication 5, caractérisé en ce que dans le cas où le nombre b est donné au préalable, on pré calcule la valeur $\lambda(b)$ et on la stocke en mémoire.

7. Dispositif électronique portable selon la revendication 5 ou 7, caractérisé en ce qu'il est constitué par une carte à puce à microprocesseur.

Fig. 1

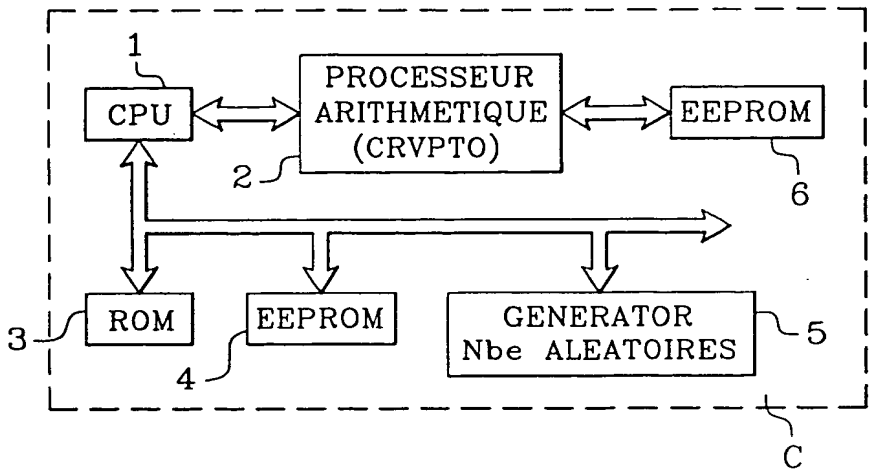
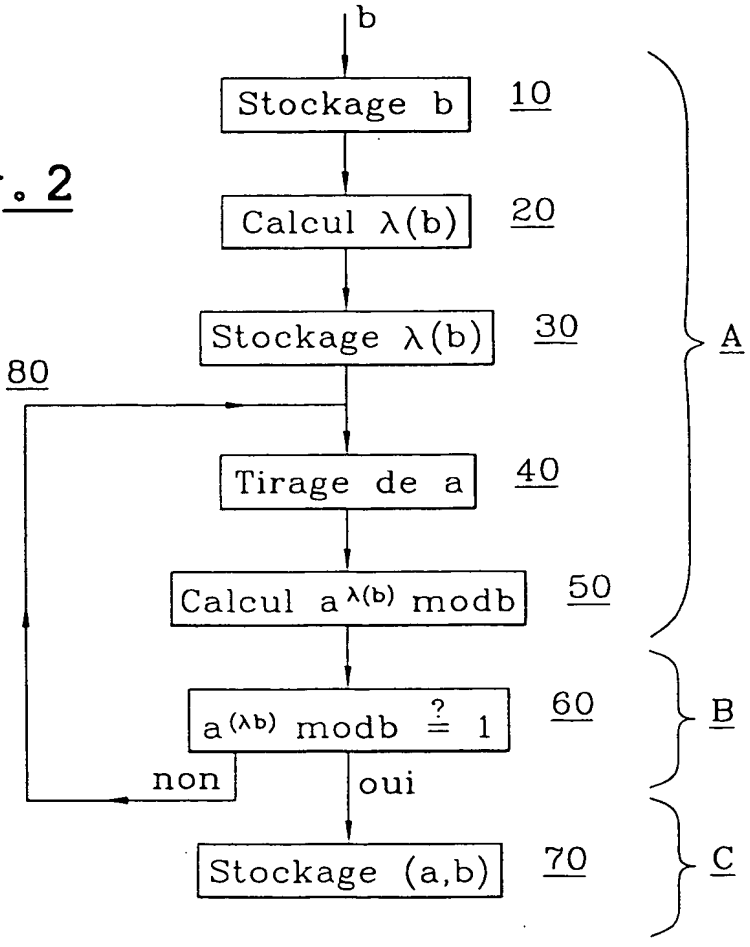

1
CPU
PROCESSEUR
ARITHMETIQUE
(CRVPTO)
2
EEPROM
6
3
ROM
EEPROM
4
GENERATOR
Nbe ALEATOIRES
5
C

Fig. 2


b
Stockage b
10
Calcul λ(b)
20
Stockage λ(b)
30
A
80
Tirage de a
40
Calcul a^λ(b) modb
50
a^(λb) modb ? = 1
60
B
non
oui
Stockage (a,b)
70
C

09/010,658